2015

(261, 105, 42) Abelian Difference Sets Do Not Exist

James Robert Hufford Jr.
Wright State University

(261, 105, 42) ABELIAN DIFFERENCE SETS DO NOT EXIST

A thesis submitted in partial fulfullment of the requirements for the degree of Master of Science

By

James R. Hufford
B.S., University of Cincinnati, 1989

2015
Wright State University

Wright State University

Graduate School

March 11, 2015

I HEREBY RECOMMEND THAT THE THESIS PREPARED UNDER MY SUPERVISION BY James R. Hufford ENTITLED (261, 105, 42) Abelian Difference Sets Do Not Exist BE ACCEPTED IN PARTIAL FULFILLMENT OF THE REQUIREMENTS FOR THE DEGREE OF Master of Science.

K.T. Arasu, Ph.D.
Thesis Director

Weifu Fang, Ph.D.
Chair, Department of Mathematics and Statistics

Committee on Final Examination

K.T. Arasu, Ph.D.

Yuqing Chen, Ph.D.

Xiaoyu Liu, Ph.D.

Robert E.W. Fyffe, Ph.D.
Vice President for Research
and Dean School of Graduate Studies

ABSTRACT

Hufford, James R.. M.S. Department of Mathematics and Statistics, Wright State University, 2015. (261, 105, 42) Abelian Difference Sets Do Not Exist.

Difference sets in the group $\mathbb{Z}_3 \times \mathbb{Z}_3 \times \mathbb{Z}_{37}$ and the group $\mathbb{Z}_3 \times \mathbb{Z}_9 \times \mathbb{Z}_7$ are known not to exist. The only open abelian case with a sylow-3 subgroup rank 2 listed in Vera-Lopez and Sanchez's [16] table is $\mathbb{Z}_3 \times \mathbb{Z}_3 \times \mathbb{Z}_{29}$. We prove for Vera-Lopez and Sanchez's table that difference sets do not exist in the open group allowing the appropriate entry to be "no". We also prove that there exist no difference sets (261, 105, 42) for any group with order 261.

Table of Contents

Contents

1 Introduction

Formalized consideration of difference sets began in the late 1930s when James Singer introduced the notion of difference sets in his paper "A theorem in finite projective geometry and some applications to number theory"[14]. In 1947 Marshall Hall introduced the concept of multipliers as applied to difference sets in his paper, "Cyclic projective planes"[9]. R.H. Bruck, in his paper, "Difference sets in a finite group"[7], extended the idea of difference sets to the finite group.

Since then the research of difference sets and their applications has exploded. Families of difference sets have been discovered through the exercise of establishing either the existence or nonexistence of particular sets using, but not exclusively, combinatorics, algebra and number theory. In their book *Design Theory*[6], Beth, Jungnickel and Lenz provide a thorough treatment of difference sets and related topics in combinatorial design theory. E.S. Lander in his 1983 book *Symmetric Designs: An Algebraic Approach*[11] used self-codes and multipliers to study abelian difference sets. He also provides the defining parameters for (v, k, λ) difference sets for $k \leq 50$ along with what was the current status of existence/nonexistence of each set. At the time of its printing, some existence/nonexistence questions remained for some $k \leq 50$ but these were answered within about 10 years. Vera-Lopez and Sanchez have since extended to $k < 150$ Lander's table. In this paper we provide a proof for nonexistence of one of the open difference sets for this extended table.

2 Difference Sets

Let G be an abelian group of order v and D be a subset of G with cardinality k. D is said to be a $(v,\ k,\ \lambda)$ difference set if the multiset $(g_1 g_2^{-1} | g_1,\ g_2 \in D,\ g_1 \neq g_2)$ contains every nonindentity element of G exactly λ times. We consider D to be abelian and cyclic when G is abelian and cyclic.

Proposition 2.1 *Let D be a (v, k, λ) difference set in G. Then k (k-1)= λ(v-1).*

Proposition 2.2 *Let D be a (v, k, λ) difference set in G. Then D' = G/D, the complement of D, is a (v, v-k, v-2k+λ) difference set in G.*

Proposition 2.3 *Let D be a (v, k, λ) difference set in G. Then, for any automorphism, σ, of G and any g ∈ G, D' = σ(D) + g = {σ(d) + g| d ∈ D, g ∈ G} is a (v, k, λ) difference set in G.*

3 Multipliers

Let D be a $(v,\ k,\ \lambda)$ difference set in G. An automorphism, σ, of G is said to be a multiplier of D if $\sigma(G) = G + g$ for some $g \in G$. An integer, t, relatively prime to the order of G, is a numeric multiplier (or multiplier) if $\sigma{:}x \to tx$ is multiplier of D.

Theorem 3.1 *Let D be a $(v,\ k,\ \lambda)$ difference set in G and p be a prime divisor of $n = k - \lambda$. Suppose that the g.c.d.$(p, v) = 1$ and $p > \lambda$. Then p is a multiplier of D.*

Theorem 3.2 *Let D be an abelian $(v,\ k,\ \lambda)$ difference set in G. Then there exists a translate of D fixed by every multiplier of D.*

Theorem 3.3 *Let D be an abelian $(v,\ k,\ \lambda)$ difference set in G and let $m > \lambda$, $m \in \mathbb{N}$, be a divisor of n such that the g.c.d.$(m, v) = 1$. Moreover, let $t \in \mathbb{Z}$ such that the g.c.d$(t, v) = 1$ satisfying the condition that for every prime p dividing m, there exists f, $f \in \mathbb{N}$, such that $t \equiv p^f (mod_{v^*})$, where v^* is an exponent of G. Then t is a multiplier of D.*

Theorem 3.4 *(Arasu and Xiang[5]). Let G be a finite group of cardinality $v{=}mn$ with exponent v^*. Let N be a normal subgroup of G cardinality n. Suppose $A{=}\mathbb{Z}G$, $A \in$ Cent($\mathbb{C}G$) satisfies $AA^{-1} = a + bN + cG$ for some a, b, and $c \in \mathbb{Z}$, $a \neq 0$. Let t be a positive integer relatively prime to v and $k_1|a$, $k_1{=}p_1^{d_1}p_2^{d_2}\cdots p_s^{d_s}$, $a_1{=}(v,k_1)$, $k_2{=}k_1/a_1$. For each p_i, $1 \leq i \leq s$, we define*

$$q_i = \begin{cases} p_i & : p_i \not| \ v^* \\ m_i & : m_i \in \mathbb{Z} | v^* = p_i^r u, (p,u) = 1, r \geq 1, (m_i, p_i) = 1, m_i \equiv p_i^f (mod_u) \end{cases} \tag{1}$$

Then for each i there exists an integer f_i such that either

$$\begin{aligned} &(1) \quad q_i^{f_1} \equiv t(mod_{v^*}) \; or \\ &(2) \quad q_i^{f_1} \equiv -1(mod_{v^*}) \end{aligned} \tag{2}$$

Also assume that one of the following conditions is satisfied:

(3) *all of the coefficients of A are nonnegative with $k_2 > b + c$ and $k_2 > c$ or*

(4) $(M(a/k_2), v) = 1$ *where M(m) is the usual multiplier function.*

Finally, assume t is a multiplier of A in G/N, then t is a multiplier of A.

4 Group Rings

Let G be a multiplicative group of order v and $\mathbb{Z}G$ denote the group ring of G over the ring of integers. A subset S of G is identified with the group ring element that is the formal sum of the elements of S (with coeffients 0 and 1). For an element, A, of $\mathbb{Z}G$ and integer t, $A^{(t)}$ denotes the image of A under the group homomorphism x to x^t extended linearly to all of $\mathbb{Z}G$.

Then addition in $\mathbb{Z}G$ is defined as follows:

$$\sum_{g\in G} a_g g + \sum_{g\in G} b_g g = \sum_{g\in G} (a_g + b_g) g \tag{3}$$

and multiplication in $\mathbb{Z}G$ is defined as:

$$\Big(\sum_{g\in G} a_g g\Big)\Big(\sum_{g\in G} b_g g\Big) = \sum_{k} \Big(\sum_{g,h;gh=k} a_g b_g g\Big) k. \tag{4}$$

Note: Here we begin an abuse of summation notation. For each subset S of G we allow S to also denote the group ring element $S = \sum_{g\in S} g$. Then, for $A = \sum_{g\in G} a_g g$ we define:

$$A^t = \sum_{g\in G} a_g g^t. \tag{5}$$

Proposition 4.1 *As defined above $\mathbb{Z}G$ is a ring with the additive identity $0_{\mathbb{Z}G} = \sum_{g \in G} 0_{\mathbb{Z}} g$ and multiplicative identity $1_{\mathbb{Z}G} = \sum_{g \in G} a_g g$ where $a_g = 1_{\mathbb{Z}}$ when $g = 1_g$ and $a_g = 0_{\mathbb{Z}}$ otherwise.*

Proposition 4.2 *Let D be a (v, k, λ) difference set in G. Then, for $D = \sum_{d \in D} d_g g$,*

$$DD^{-1} = (k - \lambda) + \lambda G. \tag{6}$$

5 Characters

Difference sets can be studied by reformulating the problem in a group algebra KG where K is some field and G is an abelian group of order v. We assume that the characteristic of K and the order of G are relatively prime or that the characteristic of K is zero. Then it is well known that the KG is semi-simple, which means that the algebra can be decomposed into two simple algebras. (Simple algebras have no non-trivial two-sided ideas.) Then there are exactly v distinct one-dimensional representations of G over the extension field, E, of K. We assume that E contains the v^{*th} root of unity where v^* is the exponent of G. These one-dimensional representations are called character homomorphisms from G to the multiplicative group of E. These characters form the character group G^* of G, and this character group is isomorphic to G.

The identity of G^* is called the principal character, χ_0, and χ_0 maps each group element to the identity. If g_i is a generator in the multiplicative group $\mathbb{Z}_{s_i}$, then the characters of G are the mapping that map g_i to a ${s_i}^{th}$ root of unity for $i = 1, 2, \ldots, v$. (This is why it is necessary to assume the existence of the v^{*th} root of unity in extension field E.) Thus, characters are mapping from G to E. These mappings can be extended linearly to an algebra homomorphism from EG into E.

Lemma 5.1 *(orthoganality relations) Let G be an abelian group of order v and exponent v^*. If the field E contains a primitive v^{*th} root of unity, then*

$$\chi(G) = \begin{cases} |G| & : \chi = \chi_0 \\ 0 & : \chi \neq \chi_0 \end{cases} \tag{7}$$

for all characters of G. Moreover, we have

$$\sum_{\chi \in G^*} \chi(g) = \begin{cases} |G| & : g = 1 \\ 0 & : g \neq 1. \end{cases} \tag{8}$$

An easy consequence of the orthogonality relations is that the character values uniquely determine the group algebra element as given in the inversion formula below.

Lemma 5.2 *(inversion formula) Let G be an abelian group of exponent v^* and let $A = \sum_{g \in G} a_g g$ be an element in the group algebra EG where E contains a primitive v^{*th} root of unity. Then*

$$a_g = \frac{1}{|G|} \sum_{\chi \in G^*} \chi(A)\chi(g^{-1}) \tag{9}$$

where the sum is over all characters χ of G.

In this paper we approach difference sets by using the sums of roots of unity as shown by Arasu, McDonough and Sehgal[2]. We follow the method outlined in the above, but the calculations are much more intensive when we consider the $|X_i| = 8$ case.

We can show that all groups with cardinality 261 are abelian with standard sylow techniques and all of these groups are isomorphic to $\mathbb{Z}_3 \times \mathbb{Z}_3 \times \mathbb{Z}_{29}$ or $\mathbb{Z}_9 \times \mathbb{Z}_{29}$. So we can prove the nonexistence of difference sets for all groups cardinality 261 by showing nonexistence in these two qroups.

6 More Tools

We use the following in our proof of the nonexistence of the subject difference sets.

Careful application of Proposition 6.1 can sometime prove or disprove the existence of a particular difference set. By this method, a group ring element can be translated and then fixed by a known multiplier to determine the existence/nonexistence of a particular difference set.

Proposition 6.1 *Let D be a (v, k, λ) difference set in an abelian group G. Let H be a subgroup of G with $[G:H] = m$. Let $G/H = \{H_i \mid 0 \leq i \leq m-1\}$ where $H_0 = H$. Let $s_i = |D \cap H_i|$. We define s_i to be the intersection numbers of D relative to H_i. Then*

$$\sum_{i=0}^{m-1} s_i = k \tag{10}$$

and

$$\sum_{i=0}^{m-1} s_i^2 = k - \lambda + \lambda|H|. \tag{11}$$

Theorem 6.2 *(Ma[12]) Let p be a prime and G be an abelian group with cyclic Sylow p-subgroups of order p^r. If $z \in \mathbb{Z}G$ satisfies $\chi(z) \equiv 0(mod_{p^r})$ for all $\chi \neq \chi_0$, then $\exists$ x_1, $x_2 \in \mathbb{Z}G$ such that $z = p^r x_1 + Px_2$ where P is the unique subgroup of cardinality p. Furthermore, if z has nonnegative coefficients, then x_1 and x_2 can be chosen to have nonnegative coefficents.*

Note: A prime p is said to be self conjugate modulo m if there exists an integer r such that $p^r \equiv -1(mod_m)$.

Theorem 6.3 *(Turyn[15]) Let ξ be a complex m^{th} root of unity and let t be an integer which is self conjugate modulo m. If $D \in \mathbb{Z}[\xi]$ and $DD^{-1} \equiv 0(mod_{t^{2a}})$ for positive integer a, then $D \equiv 0(mod_{t^a})$.*

The following theorem is a generalization of Theorem 6.2 and describes the structures of hypothetical difference sets. (Arasu and Segal[4] used this generalization to prove the nonexistence of $(189, 48, 12)$ difference sets in the group $\mathbb{Z}_3 \times \mathbb{Z}_9 \times \mathbb{Z}_7$ and $(333, 84, 21)$ difference sets in the group. $\mathbb{Z}_3 \times \mathbb{Z}_3 \times \mathbb{Z}_{37}$.

Theorem 6.4 *(Arasu and Sehgal[4]) Let D be a nontrivial (v, k, λ) difference set in an abelian group $G =< g_1 > \times < g_2 > \times H$, $|g_1| = p^a$, $|g_2| = p^b$, $1 \leq a \leq b$, $a,b \in \mathbb{N}$, p a prime, $(p, |H|)=1$. Assume that $p^{2a}|k - \lambda$ and p is self conjugate modulo exp(G). Then, for $x \in D$, $xC_p \subseteq D$ for some subgroup C_p of G, $|C_p| = p$.*

Thus, D is a union of cosets of subgroups of cardinality p.

Theorem 6.5 *(Arasu, McDonough and Sehgal[2]) Suppose n=rs where r and s are distinct primes. Let ξ be a primitive r^{th} root of unity and η be the primitive s^{th} root. Suppose that:*

$$\sum_{i=0}^{r-1} \sum_{j=0}^{s-1} a_{ij} \xi^i \eta^j = 0 \tag{12}$$

where a_{ij} is a nonnegative integer for all i and j. Then there are nonnegative integers k, m with $m < s$, such that

$$\sum_{i=0}^{r-1}\sum_{j=0}^{s-1} a_{ij} = ks + mr. \tag{13}$$

Moreover, if $k = 0$, then

$$\sum_{i=0}^{r-1}\sum_{j=0}^{s-1} a_{ij}\xi^i\eta^j = \left(\sum_{i=0}^{r-1}\xi^i\right)\left(\sum_{j=0}^{s-1} m_j\eta^j\right) \tag{14}$$

for some nonnegative integers m_j, $j = \{1, 2, \cdots, s-1\}$

7 Nonexistence of (261, 105, 42) Difference Sets

Proposition 7.1 *(261, 105, 42) difference sets do not exist in* $\mathbb{Z}_9 \times \mathbb{Z}_{29}$

Proof

Let D be a (261, 105, 42) difference set in abelian group G. Then $k - \lambda = 63 = 3^2 \times 9$. Note that $\mathbb{Z}_9$ is the sylow-3 subgroup of D and that $3^{14} \equiv -1(mod_{29})$ so that 3 is self conjugate. Let $m = 3$ and $a = 1$ in an application of theorem 6.4. Then $DD^{-1} \equiv 0(mod_{3^2}) \implies D \equiv 0(mod_3)$. By theorem 6.2, $D = 3x_1 + Px_2$ where $P = \{0, 3, 6\}$ is the unique subgroup of cardinality 3 for $x_1, x_2 \in \mathbb{Z}G$. Since the coefficients of D are 0 and 1 only, $x_1 = 0$. So $D = (1 + g^3 + g^6)x_2 \equiv 0(mod_3)$.

Now let $\chi : g^i \to {\xi_9}^i$. Then $g^3 \to {\xi_9}^3 = e^{2\pi i/3} \neq 1$. So $\chi(D)\chi(1 - g^3) = 0 \implies \chi(D)\chi(D^{-1}) = 0$ implies that D is not a difference set.

□

Proposition 7.2 *(261, 105, 42) difference sets do not exist in* $\mathbb{Z}_3 \times \mathbb{Z}_3 \times \mathbb{Z}_{29}$

Proof Let σ be the natural homomorphism from $\mathbb{Z}_3 \times \mathbb{Z}_3 \times \mathbb{Z}_{29}$ to $\mathbb{Z}_{29}$. By Theorem 3.4 (Set $G = N = \mathbb{Z}_{29}$, $A = D$, $a = 63$, $b = 0$, $c = 378$, $t = 7$, and $k_1 = 63$), we have 7 as a multiplier of D. Since 7 is a multiplier of $D \in \mathbb{Z}\mathbb{Z}_{29}$, D can be written as $\sum c_i O_i$ for $0 \leq c_i \leq 9$, $c_i \in {O_i}^{th}$ orbit of 7 in $\mathbb{Z}_{29}$ (The orbits of 7 in $\mathbb{Z}_{29}$ are the identity orbit denoted as O_0 and the 4 orbits of order 7 denoted as O_i, $1 \leq i \leq 4$, $i \in \mathbb{N}$.).

We have shown that $3^{14} \equiv -1(mod_{29})$ so 3 is self conjugate modulo 29 and we know that $3 \cdot 3|n$, $(n = k - \lambda = (105 - 42))$ so that by, Theorem 6.4, $D = \sum X_i {C_3}^i$ where the ${C_3}^i$'s are the distinct subgroups of order 3 and the X_i's are a sum of coset representatives, i.e. $X_i = (x_{i1} + x_{i2} + \cdots + x_{in}), x_{ij} \in {C_3}^i \times \mathbb{Z}_{29}$, $1 \leq j \leq n$, $j \in \mathbb{Z}$. Notice that when $i \neq j$, $x_{im}x_{jn}^{-1} \notin \mathbb{Z}_3 \times \mathbb{Z}_3$. ($x_{im}x_{jn}^{-1} \in \mathbb{Z}_3 \times \mathbb{Z}_3$ implies that $D = \cdots x_{im}{C_3}^i + x_{jn}{C_3}^j \cdots$ which contradicts D having coefficients 0 and 1 only.) Also, since $|{C_3}^i| = 3$, any intersection number, $|D \cap \mathbb{Z}_3 \times \mathbb{Z}_3|$, must be a multiple of 3.

We can find the intersection numbers with $H = \mathbb{Z}_3 \times \mathbb{Z}_3$ by Proposition 6.1. Since D is a combination of O_i's, $0 \leq i \leq 4$, there must be 4 size 7 sets of intersection numbers $mod_{\mathbb{Z}_3 \times \mathbb{Z}_3}$ that are the same and correspond to $O_i \neq O_0$. That allows us to rewrite the intersection summations as

$$\sum_i s_i = k = s_0 + 7s_1 + 7s_2 + 7s_3 + 7s_4 = 105 \tag{15}$$

and

$$\sum_i s_i^2 = k - \lambda + \lambda|H| = {s_0}^2 + 7{s_1}^2 + 7{s_2}^2 + 7{s_3}^2 + 7{s_4}^2 = 105 - 42 + 42(9) = 441 \tag{16}$$

where $0 \leq s_i \leq 9$. Since $3|s_i$, we can rewrite s_i as $3t_i$ which gives us

$$t_0 + 7t_1 + 7t_2 + 7t_3 + 7t_4 = 35 \tag{17}$$

and

$${t_0}^2 + 7{t_1}^2 + 7{t_2}^2 + 7{t_3}^2 + 7{t_4}^2 = 49 \tag{18}$$

where $0 \leq t_i \leq 3$. The solution to (17) and (18), $\{t_0, t_1, t_2, t_3, t_4\} = \{\emptyset, 1, 1, 1, 2\}$, implies that $\{s_0, s_1, s_2, s_3, s_4\} = \{\emptyset, 3, 3, 3, 6\}$ where $\emptyset$ as s_0 implies that no element of the identity coset appears in the intersection numbers and 4 intersection numbers appear 7 times across the orbits of $\mathbb{Z}_{29}$.

As noted before, because $i \neq j \Rightarrow x_{im}{x_{jn}}^{-1} \notin \mathbb{Z}_3 \times \mathbb{Z}_3$, we know that in any coset of $\mathbb{Z}_3 \times \mathbb{Z}_3$ there are a certain number of copies of ${C_3}^i$ for any $i \neq j$. This fact, along with $\mathbb{Z}_3 \times \mathbb{Z}_3$ intersection numbers, gives us 21 distinct cosets of $\mathbb{Z}_3 \times \mathbb{Z}_3$ with exacty one ${C_3}^i$ for some i and 7 distinct cosets of $\mathbb{Z}_3 \times \mathbb{Z}_3$ with two copies of ${C_3}^i$ for some i.

Now we can write the intersection equations with $H = {C_3}^i$ as:

$$b + 2c + 3d = 105 \tag{19}$$

and

$$b + 4c + 9d = 105 - 42 + 42(3) = 189 \tag{20}$$

where b, c and d are the number of s_i's equal to 1, 2 and 3, respectively.

Consider that $d = |X_i|$ is the number of coset representatives in X_i, that $c = 3$ multiplies the number cosets of $\mathbb{Z}_3 \times \mathbb{Z}_3$ containing two copies of ${C_3}^{j \neq i}$, and that $b = 3$ multiplies the number cosets of $\mathbb{Z}_3 \times \mathbb{Z}_3$ containing one copy of ${C_3}^{j \neq i}$. Also consider that, since there are at most 7 cosets of ${C_3}^{j \neq i}$, $c \leq 3 \cdot 7 = 21$. Now, subtracting (19) from (20) we get $c + 3d = 42$ which implies that $7 \leq |X_i| \leq 14$, which implies that there are at least 7 cosets of ${C_3}^i$ for each i and that the number of cosets of $\mathbb{Z}_3 \times \mathbb{Z}_3$ with two copies of $C_3^{j \neq i}$ is $14 - |X_i|$. This means that the number of leftover ${C_3}^i$ cosets with two copies is $7 - (14 - |X_i|) = |X_i| - 7$. So, if $|X_i| = 7$, there will be 7 distinct cosets of $\mathbb{Z}_3 \times \mathbb{Z}_3$ containing one copy ${C_3}^i$. Then, for each n, $n \in \mathbb{N}$, there will be $7 + n$ distinct cosets of $\mathbb{Z}_3 \times \mathbb{Z}_3$, which contain two copies of ${C_3}^i$, and $7 - n$ cosets that contain single copies of ${C_3}^i$.

Again rewriting the intersection equations with $H = {C_3}^i \times \mathbb{Z}_{29}$, we have:

$$s_0 + s_1 + s_2 = 105 \tag{21}$$

and

$$s_0{}^2 + s_1{}^2 + s_2{}^2 = 105 - 42 + 42(3)(29) = 3717. \tag{22}$$

Solving (21) and (22) for s_2 gives us:

$$s_2 = \frac{\pm\sqrt{-3s_0{}^2 + 210s_0 - 3591} - s_0 + 105}{2} \tag{23}$$

Notice that s_2 is non-imaginary only when $30 \leq s_0 \leq 40$. So we can discover all values for s_2 in which $s_2 \in \mathbb{Z}$. So $\{s_0, s_1, s_2\}$=$\{30, 36, 39\}$ or $\{s_0, s_1, s_2\}$=$\{31, 34, 39\}$ are the only solutions. Now, every coset of $C_3{}^{j\neq i}$ contributes exactly one element to each coset of H. This means that we can use the number of $C_3{}^{j\neq i}$ cosets to determine some parameters of the cosets of $C_3{}^i$. Above we found the number of $C_3{}^{j\neq i}$ cosets with one copy of in $\mathbb{Z}_3 \times \mathbb{Z}_3$ to be twice the number of $C_3{}^{j\neq i}$ with two copies in $\mathbb{Z}_3 \times \mathbb{Z}_3$ so $\frac{2c+b}{3} = \frac{2c+105-2c-3d}{3} = \frac{105-3d}{3} = 35 - |X_i|$. Each of the $35 - |X_i|$ cosets of $C_3{}^{j\neq i}$ contribute a total $35 - |X_i|$ elements to each s_i so that $\{30, 36, 39\}$=$\{t_0 + 35 - |X_i|, t_1 + 35 - |X_i|, t_2 + 35 - |X_i|\}$ or $\{31, 34, 40\}$=$\{t_0 + 35 - |X_i|, t_1 + 35 - |X_i|, t_2 + 35 - |X_i|\}$. The remaining t_i's must come from the cosets of $C_3{}^i$ and, therefore, must be multiples of 3. Since we have that $t_0 + 35 - |X_i| \equiv 30 (mod_3)$ or $t_0 + 35 - |X_i| \equiv 31 (mod_3)$, we have $|X_i| \equiv 1 (mod_3)$ or $|X_i| \equiv 2 (mod_3) \Rightarrow 3 \nmid |X_i|$. So we have that $|X_i| = 7, 8, 10, 11, 13$ or 14. Given these possibilities for $|X_i|$ and the fact that $\sum_i |X_i| = \frac{k}{3} = 35$, we have the following possibilities for $\{|X_1|, |X_2|, |X_3|, |X_4|\}$: $\{14, 7, 7, 7\}$, $\{13, 8, 7, 7\}$, $\{11, 10, 7, 7\}$, $\{11, 8, 8, 8\}$ or $\{10, 10, 8, 7\}$. Notice that in each of these possibilities $|X_i| = 7$ or $|X_i| = 8$.

We exploit this fact to break down our proof into the two cases ($|X_i| = 7$ or $|X_i| = 8$) and use the method prescribed by Arasu, McDonought, and Sehgal[2] to find the distribution of X_i's across $C_3{}^i \times \mathbb{Z}_{29}$. By proving that the two cases cannot exist, we prove the non-existence of the subject difference set.

Let χ be a character in G^* such that $\chi|G \neq \chi_0$, $\chi|\mathbb{Z}_3 \times \mathbb{Z}_3 \neq \chi_0$ and $\chi|C_3{}^i = \chi_0$.

It is well known that $\chi({C_3}^i) = 0$, so

$$\chi(D) = \chi(X_1C_3^1 + X_2C_3^2 + X_3C_3^3 + X_4C_3^4) = \chi(X_i{C_3}^i) = 3\chi(X_i) \tag{24}$$

and

$$\chi(D)\overline{\chi(D)} = k - \lambda = 105 - 42 = 63 = 9\chi(X_i) \tag{25}$$

Let $\alpha = \chi(X_i)$. We observe that $\alpha\bar{\alpha} = 7$.

Case: $|X_i| = 7$. Let $\alpha = \sum_{i=0}^{6} \xi^{u_i}$ for suitable integers $0 \leq u_i \leq 87$ and ξ the 87^{th} root of unity. We can now rewrite $\alpha\bar{\alpha} = 7$ as

$$\sum_{\substack{i \neq j \\ 0 \leq i \leq 6 \\ 0 \leq j \leq 6}} \xi^{u_i - u_j} = 0 \tag{26}$$

Now we apply Theorem 6.5 with $r = 3$ and $s = 29$ which gives us $(29)k + (3)m = 7 \cdot 6 = 42$. Then $k = 0$ and $m = 14$ implies that:

$$\sum_{\substack{i \neq j \\ 0 \leq i \leq 6 \\ 0 \leq j \leq 6}} \xi^{u_i - u_j} = \left(\sum_{i=0}^{2} \xi^{29i}\right)\left(\sum_{m=1}^{14} \xi^{3j_m}\right) \tag{27}$$

for suitable integers $j_m, 1 \leq m \leq 14$.

Now, we found the intersection numbers $(mod_{{C_3}^i \times \mathbb{Z}_{29}})$ to be $\{30, 36, 39\}$ or $\{31, 34, 40\} = \{t_0+35-|X_i|, t_1+35-|X_i|, t_2+35-|X_i|\} = \{t_0+28, t_1+28, t_2+28\}$. Since $3|t_i$, we have $\{t_0, t_1, t_2\} = \{3, 6, 12\}$, which implies that in X_i we have a distribution of $\{3, 6, 12\} \equiv \{1, 2, 4\}(mod_{<\xi^3>})$ in ${C_3}^i \times \mathbb{Z}_{29}$. This distribution applied to α means that the distribution of elements contributing to α is $\{1, 2, 4\}(mod_{<\xi^3>})$. By conjugating and multiplying by a suitable root of unity, we argue that the distribution is exactly 1, 2 and 4 across each coset and that $u_0 = 3v_0$, $u_{1,2} = 3v_{1,2} + 1$ and $u_{3,4,5,6} = 3v_{3,4,5,6} + 2$ for suitable integers $v_0, \cdots, v_6$.

If we consider the summation equations above as lists, we will find that they are equivalent for the 42 elements (working in $\mathbb{Z}/29\mathbb{Z}$ since the elements occur 3 times across each coset ($mod_{<\xi^3>}$)). To list the exponents that are congruent to $0(mod_3)$ we use

$$3(v_i - v_j) \text{ where } i \neq j \text{ and either } 1 \leq i, j \leq 2 \text{ or } 3 \leq i, j \leq 6$$

or, equivalently,

$$3j_m \text{ where } m = 1, \cdots, 14.$$

To list the exponents congruent to $1(mod_3)$ we use

$$3(v_i - v_0) + 1 \text{ where } 1 \leq i \leq 2,$$

$$3(v_i - v_j) + 1 \text{ where } 3 \leq i \leq 6 \text{ and } 1 \leq j \leq 2$$

$$3(v_0 - v_j) - 2 \text{ where } 3 \leq j \leq 6$$

or, equivalently,

$$3j_m + 29 \text{ where } m = 1, \cdots, 14.$$

These two lists are equivalent (mod_{29}), so we can divide each by $3(mod_{29})$ to get

$$v_i - v_j \text{ where } i \neq j \text{ and either } 1 \leq i, j \leq 2 \text{ or } 3 \leq i, j \leq 6$$

which can be rewritten as

$$v_i - v_0 + 10 \text{ where } 1 \leq i \leq 2,$$

$$v_i - v_j + 10 \text{ where } 3 \leq i \leq 6 \text{ and } 1 \leq j \leq 2 \ ,$$

and

$$v_0 - v_j + 9 \text{ where } 3 \leq j \leq 6$$

in $\mathbb{Z}/\mathbb{Z}_{29}$.

At this juncture we make the following substitutions for convenience:

$$w_i = v_i - v_0 + 10 \text{ when } i = 1, 2$$

and

$$w_i = -(v_0 - V_i + 9) \text{ when } i = 3, 4, 5, 6$$

The two lists then become

$$w_i - w_j \text{ where } i \neq j \text{ and either } 1 \leq i, j \leq 2 \text{ or } 3 \leq i, j \leq 6$$

which can be rewritten as

$$w_i \text{ where } 1 \leq i \leq 2,$$

$$w_i - w_j \text{ where } 3 \leq i \leq 6 \text{ and } 1 \leq j \leq 2,$$

and

$$-w_i \text{ where } 3 \leq j \leq 6$$

Now, let $S_n = {w_3}^n + {w_4}^n + {w_5}^n + {w_6}^n$, T_n be the elementary symmetric function of $0, 0, w_3, w_4, w_5, w_6$, and $T_{k(a,b,c,d)}$ be all possible sums with $k \leq 4$ distinct terms from the set $\{w_3, w_4, w_5, w_6\}$ raised to the powers a, b, c and d. For example

$$T_{2(2,2)} = {w_3}^2{w_4}^2 + {w_3}^2{w_5}^2 + {w_3}^2{w_6}^2 + {w_4}^2{w_5}^2 + {w_4}^2{w_6}^2 + {w_5}^2{w_6}^2$$

$$T_{4(7,1,1,1)} = {w_3}^7 w_4 w_5 w_6 + w_3 {w_4}^7 w_5 w_6 + w_3 w_4 {w_5}^7 w_6 + w_3 w_4 w_5 {w_6}^7$$

$$T_3 = w_3 w_4 w_5 + w_3 w_4 w_6 + w_3 w_5 w_6 + w_4 w_5 w_6$$

Note that $S_n = T_{1(n)} = T_{4(n,0,0,0)}$.

It can be shown that all $T_{4(a,b,c,d)}$ can be represented in terms of S_n's in the following manner (Assume $a \geq b \geq c \geq d$):

If $a \neq 0$ and $b = c = d = 0$, then

$$T_{4(a,b,c,d)} = S_a$$

If $a, b \neq 0$ and $c = d = 0$, then

$$T_{4(a,b,c,d)} = \begin{cases} {}^1/_2({S_a}^2 - S_{2a}) & \text{if } a = b \\ S_a S_b - S_{a+b} & \text{if } a \neq b \end{cases}$$

If $a, b, c \neq 0$ and $d = 0$, then

$$T_{4(a,b,c,d)} = \begin{cases} T_{2(a,b)}S_c - T_{2(a+c,b)} - 2T_{2(a,b+c)} & \text{if } a > b > c \text{ and } a = b + c \\ T_{2(a,b)}S_c - T_{2(a+c,b)} - T_{2(a,b+c)} & \text{if } a > b > c \text{ and } a \neq b + c \\ T_{2(a,a)}S_c - T_{2(a+c,a)} & \text{if } a = b > c \\ T_{2(b,b)}S_a - T_{2(a+b,b)} & \text{if } a > b = c \\ (T_{2(b,b)}S_b - T_{2(2b,b)})/3 & \text{if } a = b = c \end{cases}$$

If $a, b, c, d \neq 0$ then,

$$T_{4(a,b,c,d)} = T_{3(a-d,b-d,c-d)}(S_4 - {S_1}^4 + 4T_{2(3,1)} + 6T_2(2,2) + 12T_{3(2,1,1)})/(-24)$$

When we equate the sums of the n^{th} powers of the elements of the two lists we can write:

$$((-1)^n + 1)\left[(w_1 - w_2)^n + 3S_n + \sum_{i=1}^{n/2}(-1)^i\, n\binom{n}{i}T_{2(n-i,i)}\right] =$$

$$w_1^n + w_2^n + (-1)^n\, S_n + 2S_n + \left(\sum_{i=1}^{n-1}(-1)^{\ i}\, n\binom{n}{i}\left({w_1}^i + {w_2}^i\right) S_{n-i}\right) + 4\,(-1)^n\,(w_1^n + w_2^n)$$

The above equation can then be used by induction to find each S_n for $n = 1, \cdots, 6$. The following equations were produced (mod_{29}):

$$T_1 = w_1 + w_2 + w_3 + w_4 = 3w_1 + 3w_2$$

$$T_2 = w_3w_4 + w_3w_5 + w_3w_6 + w_4w_5 + w_5w_6 = 3{w_1}^2 + 3{w_2}^2 + 12w_1w_2$$

$$T_3 = w_3w_4w_5 + w_3w_4w_6 + w_3w_5w_6 + w_4w_5w_6 = {w_1}^3 + {w_2}^3 + 12{w_1}^2w_2 + 12{w_2}^2w_1$$

$$T_4 = w_3w_4w_5w_6 = 15{w_1}^3w_2 + 15w_1{w_2}^3{+}5{w_1}^2{w_2}^2$$

$$T_5 = 0 = {w_1}^4w_2 + w_1{w_2}^4{+}10{w_1}^3{w_2}^2{+}10{w_1}^2{w_2}^3$$

$$T_6 = 0 = {w_1}^5w_2 + w_1{w_2}^5{+}15{w_1}^4{w_2}^2{+}15{w_1}^2{w_2}^4{+}8{w_1}^3{w_2}^3$$

Notice that T_5 factors into $w_1w_2(w_1 + w_2)({w_1}^2{+}9w_1w_2 + {w_2}^2)$, which implies that w_1, w_2, $w_1 + w_2$, or ${w_1}^2{+}9w_1w_2 + {w_2}^2 = 0$. If $w_1 = -w_2$, then $T_6 = 0 = 20{w_2}^6 \Rightarrow$ $w_1 = w_2 = 0$. If ${w_1}^2{+}9w_1w_2{+}{w_2}^2{=}\ 0$, then $0 = T_6 - ({w_1}^2{+}9w_1w_2{+}{w_2}^2)^2 = 3{w_1}^3w_2 +$ $17{w_1}^2{w_2}^2{+}3w_1{w_2}^3$ so that either w_1, w_2, or $(3{w_1}^2{+}17w_1w_2 + 3{w_2}^2) - 3({w_1}^2{+}9w_1w_2 +$ ${w_2}^2) = 19w_1w_2 = 0$, all of which imply that w_1 or w_2 is zero.

In any case, w_1 or w_2 is zero, so we can assume without loss of generality that $w_1 = 0$, which implies that $T_4 = 0$, which implies that w_3, w_4, w_5 or $w_6 = 0$. Again, we can assume that $w_3 = 0$ so that the solutions for equations T_1, T_2 and T_3 for congruence occur when $x^3 - 3w_2x^2 + 3w_2x - {w_2}^3{=}\ 0 \Rightarrow w_4 = w_5$.

However, $w_4 = w_5 \Rightarrow v_4 = v_5 \Rightarrow u_4 = u_5$, and this contradicts the fact the X_i has coefficients only 1 and 0 in $C_3^i \times \mathbb{Z}_{29}$. So $|X_i| \neq 7$.

Case: $|X_i|{=}\ 8$. Let $\alpha = \sum_{i=0}^{7} \xi^{u_i}$ for suitable integers $0 \leq u_i \leq 87$ and ξ the 87^{th} root of unity. We can now rewrite $\alpha\bar{\alpha} = 7$ as

$$\sum_{\substack{i \neq j \\ 0 \leq i \leq 7 \\ 0 \leq j \leq 7}} \xi^{u_i - u_j} + 1 = 0 \tag{28}$$

Now we apply Theorem 6.5 with $r = 3$ and $s = 29$. We have that $(29)k + (3)m = 57$, and, with $k = 0$ and $m = 19$, that implies that

$$\sum_{\substack{i \neq j \\ 0 \leq i \leq 7 \\ 0 \leq j \leq 7}} \xi^{u_i - u_j} + 1 = \left(\sum_{i=0}^{2} \xi^{29i}\right)\left(\sum_{m=1}^{19} \xi^{3j_m}\right) \tag{29}$$

for suitable integers $j_m, 1 \leq m \leq 19$.

Now, we find the intersection numbers ($mod_{C_3^i \times \mathbb{Z}_{29}}$) to be $\{30, 36, 39\}$ or $\{31, 34, 40\}$=$\{t_0 + 35 - |X_i|, t_1 + 35 - |X_i|, t_2 + 35 - |X_i|\}$=$\{t_0 + 27, t_1 + 27, t_2 + 27\}$. Since $3|t_i$, we have $\{t_0, t_1, t_2\}$=$\{3, 9, 12\}$, which implies that in X_i we have a distribution of $\{3, 8, 12\} \equiv \{1, 3, 4\}(mod_{<\xi^3>})$ in $C_3^i \times \mathbb{Z}_{29}$. This distribution applied to α means that the distribution of elements contributing to α is $\{1, 3, 4\}(mod_{<\xi^3>})$. By conjugating and multiplying by a suitable root of unity, we argue that the distribution is exactly 1, 3 and 4 across each coset and that $u_0 = 3v_0$, $u_{1,2,3} = 3v_{1,2,3}+1$ and $u_{4,5,6,7} = 3v_{4,5,6,7}+2$ for suitable integers $v_0, \cdots, v_7$.

If we consider the summation equations above as lists, we will find that they are equivalent for the 57 elements (working in $\mathbb{Z}/\mathbb{Z}_{29}$, since the elements occur 3 times across each coset $(mod_{<\xi^3>})$. To list the exponents that are congruent to $0(mod_3)$, we use

$$3(v_i - v_j) \text{ where } i \neq j \text{ and either } 1 \leq i, j \leq 3 \text{ or } 4 \leq i, j \leq 7$$

or, equivalently,

$$3j_m \text{ where } m = 1, \cdots, 19.$$

To list the exponents congruent to $1(mod_3)$ we use

$$3(v_i - v_0) + 1 \text{ where } 1 \leq i \leq 3,$$

$$3(v_i - v_j) + 1 \text{ where } 4 \leq i \leq 7 \text{ and } 1 \leq j \leq 3$$

$$3(v_0 - v_j) - 2 \text{ where } 4 \leq j \leq 7$$

or, equivalently,

$$3j_m + 29 \text{ where } m = 1, \cdots, 19.$$

These two lists are equivalent (mod_{29}), so we can divide each by $3(mod_{29})$ to get

$$\{v_i - v_j \text{ where } i \neq j \text{ and either } 1 \leq i, j \leq 3 \text{ or } 4 \leq i, j \leq 7\}$$

which can be rewritten as

$$\{v_i - v_0 + 10 \text{ where } 1 \leq i \leq 3,$$

$$v_i - v_j + 10 \text{ where } 4 \leq i \leq 7 \text{ and } 1 \leq j \leq 3 \ ,$$

and

$$v_0 - v_j + 9 \text{ where } 4 \leq j \leq 7\}$$

in $\mathbb{Z}_{29}$.

Again, we make the following substitutions for convenience:

$$w_i = v_i - v_0 + 10 \text{ when } i = 1, 2, 3$$

and

$$w_i = -(v_0 - V_i + 9) \text{ when } i = 4, 5, 6, 7$$

The two lists then become

$$\{w_i - w_j \text{ where } i \neq j \text{ and either } 1 \leq i, j \leq 3 \text{ or } 4 \leq i, j \leq 7\}$$

which can be rewritten as

$$\{w_i \text{ where } 1 \leq i \leq 3,$$

$$w_i - w_j \text{ where } 4 \leq i \leq 7 \text{ and } 1 \leq j \leq 3,$$

and

$$w_i \text{ where } 4 \leq j \leq 7\}$$

Now, let $S_n = {w_4}^n + {w_5}^n + {w_6}^n + {w_7}^n$, T_n be the elementary symmetric function of $w_4, w_5, w_6, w_7, 0, 0$, and $T_{k(a,b,c,d)}$ be all possible sums with k distinct terms from the set $\{w_4, w_5, w_6, w_3\}$ raised to the powers a, b, c and d.

When we equate the sums of the n^{th} powers of the elements of the two lists we can write:

$$((-1)^n+1)\left[(w_1-w_2)^n+(w_3-w_2)^n+(w_3-w_1)^n+3S_n+\left(\sum_{i=1}^{n/2}(-1)^i\,n\binom{n}{i}T_{2(n-i,i)}\right)\right]=$$

$$w_1{}^n+w_2{}^n+w_3{}^n+(-1)^n\,S_n+3S_n+\Big(\sum_{i=1}^{n-1}(-1)^i\,n\tbinom{n}{i}\big(w_1{}^i+w_2{}^i+w_3{}^i\big)S_{n-i}\Big)+$$
$$4\,(-1)^n\,(w_1{}^n+w_2{}^n+w_3{}^n)$$

The above equation can then be used by induction to find each S_n for $n=1,\cdots,6$. The following equations were produced (mod_{29}):

$$T_5=0=\underline{S}_5+26\underline{T}_{2(4)}+2\underline{T}_{2(3,2)}+27\underline{T}_{3(3,1,1)}+28\underline{T}_{3(2,2,1)}$$

$$T_6=0=\underline{S}_6+19\underline{T}_{2(5)}+2\underline{T}_{2(4,2)}+6\underline{T}_{3(4,1,1)}+14\underline{T}_{2(3,3)}+17\underline{T}_{3(3,2,1)}+16\underline{T}_{3(2,2,2)}$$

where $\underline{S}$ and $\underline{T}$ permute the set $\{w_1,w_2,w_3\}$.

We now have two equations relating w_1,w_2, and $w_3\in\mathbb{Z}_{29}$. We can arbitrarily assume that $w_1=0$ and then solve for the solutions of the form $\{0,x,y\}$, which we did by hand. By the same logic we can assume that $w_1=1$ and then solve for the solutions of the form $\{1,x,y\}$. This, however, can be completely tedious, so we used a computer in the search space $|\mathbb{Z}_{29}\times\mathbb{Z}_{29}|=841$.

The only solutions of the systems of equations T_5 and T_6 are

$$w_1=0,\ w_2=w_3$$

or

$$w_2=0,\ w_1=w_3$$

or

$$w_3=0,\ w_1=w_3.$$

We may assume that $w_1 = 0$ and $w_2 = w_3 \Rightarrow v_2 = v_3 \Rightarrow u_2 = u_3$, and this contradicts the fact the X_i has coefficients only 1 and 0 in ${C_3}^i \times \mathbb{Z}_{29}$. So $|X_i| \neq 8$. Since no $|X_i| = 7$ or 8, there are no difference sets $(261, 105, 42)$ in $\mathbb{Z}_3 \times \mathbb{Z}_3 \times \mathbb{Z}_{29}$.

□

8 References

References

[1] KT Arasu. *Quotient Sets, homomorphic images and multipliers*. PhD thesis, Ohio State University, 1983.

[2] KT Arasu, TP McDonough, and SK Sehgal. Sums of roots of unity in group theory. *World Scientific*, 6(20), 1993.

[3] KT Arasu and DK Ray-Chaudhuri. Multiplier theorem for a difference list. *ARS Combinatoria*, 22(119-137), 1986.

[4] KT Arasu and Surinder K Sehgal. Difference sets in abelian groups ofp-rank two. *Designs, Codes and Cryptography*, 5(1):5–12, 1995.

[5] KT Arasu and Qing Xiang. Multiplier theorems. *Journal of Combinatorial Designs*, 3(4):257–268, 1995.

[6] Thomas Beth, Dieter Jungnickel, and Hanfried Lenz. *Design theory*, volume 69. Cambridge University Press, 1999.

[7] Richard H Bruck. Difference sets in a finite group. *Transactions of the American Mathematical Society*, pages 464–481, 1955.

[8] Jeffrey H Dinitz and Douglas R Stinson. *Contemporary design theory: A collection of Surveys*, volume 26. John Wiley & Sons, 1992.

[9] Marshall Hall Jr et al. Cyclic projective planes. *Duke Mathematical Journal*, 14(4):1079–1090, 1947.

[10] Dieter Jungnickel and Alexander Pott. Difference sets: An introduction. In *Difference sets, sequences and their correlation properties*, pages 259–295. Springer, 1999.

[11] Eric S Lander. *Symmetric designs: an algebraic approach*. Number 74. Cambridge University Press, 1983.

[12] Siu-lun Ma. *Polynomial addition sets*. PhD thesis, University of Hong Kong, 1985.

[13] Henry Berthold Mann. *Addition theorems: The addition theorems of group theory and number theory*. RE Krieger Publishing Company, 1976.

[14] James Singer. A theorem in finite projective geometry and some applications to number theory. *Transactions of the American Mathematical Society*, 43(3):377–385, 1938.

[15] Richard Turyn. Character sums and difference sets. *Pacific Journal of Mathematics*, 15(1):319–346, 1965.

[16] A Vera Lopez and MA Garcia Sanchez. On the existence of abelian difference sets with $100 < k \leq 150$. *Journal of Combinatorial Mathematics and Combinatorial Computing*, 23:97–112, 1997.